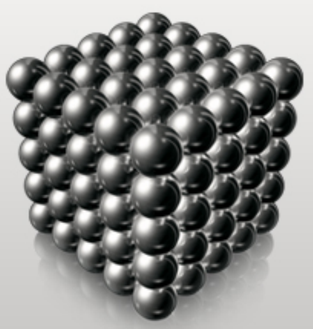
Network Authentication

Session 636

These are confidential sessions—please refrain from filming or taking pictures.



Enterprise IT

Network Authentication

Eric Clements
Directory Service Engineer

http://developer.apple.com/wwdc2005/

What You'll Learn

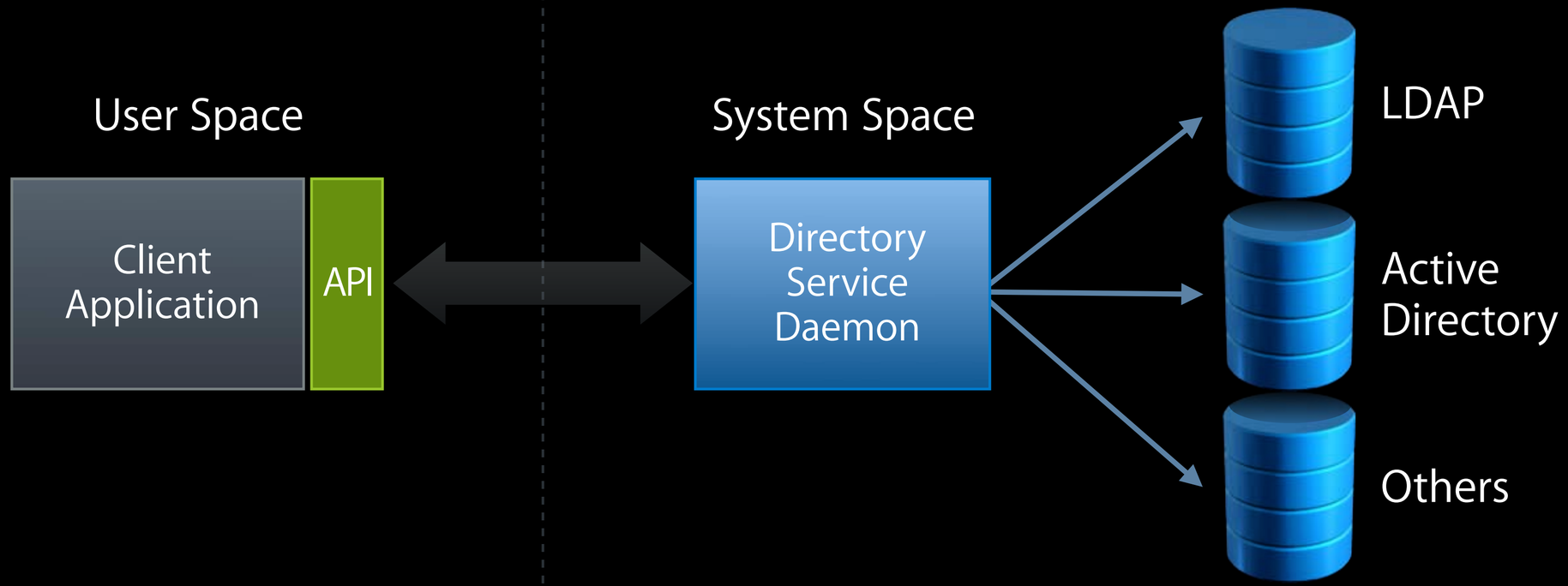
- Brief overview of Open Directory
- Apple's position on authentication
- Discussion on authentication
- Code examples for common authentication types
- Q&A

Open Directory Overview

- Open Directory provides API abstractions for read/write directory data
- Open Directory also provides authentication abstractions
  - Password-based authentication
  - Challenge/Response (NTLM, CRAM-MD5)

Technology Framework

- Directory independent APIs for interacting with various Directory Systems
- Daemon process handles client requests



Apple's Position on Authentication

- Apple offers full support for legacy password methods
- Apple is aggressively pursuing Kerberos for network authentication
  - Interoperable across multiple OS platforms
- We have added Kerberos support to the majority of our software
  - Encourage developers to do the same

Panther/Tiger Mac OS X Server

- Panther/Tiger Servers are deployed at your customer sites with Open Directory already setup
- Open Directory supports both Password-based and Kerberos-based authentication
- Applications should use password and/or Kerberos authentication
  - Very few infrastructure or deployment barriers
- This session will give you sample code for your software to integrate with Open Directory
  - This sample code will also work at Active Directory Sites

How Do I Authenticate a User?

- Various frameworks available to authenticate a user
  - Security.framework
  - DirectoryService.framework
  - PAM-based authentication
- Nearly all desktop applications should use Security.framework
- Server-based applications should use
  - DirectoryService.framework or PAM for password-based authentication
  - GSSAPI for Kerberos-based authentication

Authentication vs. Authorization

- Authentication is about proof of identity—who is the user attempting to perform an operation
- This is not authorization!
  - Use the identity established via authentication to consult a configuration for authorization
  - Use configuration files or well known group membership check
  - Necessary to scale and fit your service into a large infrastructure
  - Mac OS X Tiger Server supports Service Access Control Lists (SACLs)

Open Directory Headers

- DirectoryService.framework encompasses all APIs
  - `#include <DirectoryService/DirectoryService.h>`
- Authentication API
  - Multiple authentication methods
  - Authentication support varies by plugin and directory
  - Extensible for future methods

```
tDirStatus dsDoDirNodeAuth (tDirNodeReference  inDirNodeReference,
                            tDataNodePtr       inDirNodeAuthName,
                            dsBool             inDirNodeAuthOnlyFlag,
                            tDataBufferPtr     inAuthStepData,
                            tDataBufferPtr     outAuthStepDataResponse,
                            tContextData       *inOutContinueData )
```

Kerberos

- Ticket-based single sign-on technology
- Adopted by Apple, Microsoft, Novell, and others
- Has become an industry standard for single sign-on
- Supports packet encryption, packet signing, and mutual authentication
- GSSAPI is a common method used for network protocols
  - SPNEGO and SASL use encapsulated GSSAPI tokens

Kerberos Considerations

- Ensure the server has matching forward and reverse DNS entries
- Determine if application will run as root
  - Needed in order to use keytab
- Determine if GSSAPI will satisfy requirements
- Service keys may differ between platforms
  - HTTP/server.domain.com@REALM
  - http/server.domain.com@REALM

Typical Flow of Authentication

Password-based

- Get name and password
- Lookup user in Directory
- Authenticate User with `dsDoDirNodeAuth()`
- Check Authorization
- Allow/Deny Access

Kerberos-based

- Verify Service Ticket
- Lookup user in Directory
- Check Authorization
- Allow/Deny Access

Code Examples and Demo

http://developer.apple.com/wwdc2005/

More Information

http://developer.apple.com/wwdc2005/

Documentation, Sample Code, and Other Resources

http://developer.apple.com/wwdc2005/

Who to Contact

Skip Levens
Server Technology Manager
skip@apple.com

Q&A

http://developer.apple.com/wwdc2005/

WWDC2005

Worldwide Developers Conference